



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	M-11702 US	6041

32605 7590 02/26/2007
MACPHERSON KWOK CHEN & HEID LLP
2033 GATEWAY PLACE
SUITE 400
SAN JOSE, CA 95110

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/927,928

Applicant(s)

FAN ET AL.

Examiner

Tamara Teslovich

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 November 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6, 8-11, 15-17, 20, 25-27, 29-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892), | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This Office Action is in response to the Applicant's Remarks and Amendments filed November 20, 2006.

Claims 5, 7, 12-14, 18-19, 21-24, and 28 remain canceled.

Claims 1, 10, and 29 have been amended

Claims 1-4, 6, 8-11, 15-17, 20, 25-27, and 29-35 are pending.

Response to Arguments

Applicant's arguments filed February 28, 2006 have been fully considered but they are not persuasive.

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant argues on pages 8-10 that his claim does not in fact teach the dedicated link disclosed by Droge. If it is the Applicant's intention to argue that Droge fails to teach forwarding a once encrypted packet over a communication link, then he must do so. However, as it stands, it is clear that Droge transmits his once encrypted packet over a dedicated link, wireless or wired. Although specifically teaches the use of a dedicated line to improve security, there is nothing within the Applicant's claims that

Art Unit: 2137

rules out the use of a dedicated line. Applicant's citation of paragraph 10 of Droge's specification also fails to support Applicant's contentions seeing as paragraph 10 appears within Droge's related art description and described systems other than those taught by Droge. If it is the Applicant's intention to show that Droge fails to disclose the limitations of the instant application, the Examiner would like to request that the Applicant point to specific limitations and those specific areas within Droge's description which are in conflict with those limitations. Once again, it is clear from paragraphs 36-37 and 42 of Droge that the transmission between the first and second interface devices could very well comprise a wired or wireless network (par 36), and that the second interface device may comprise a transmission mechanism for the transmission of the data, now only once encrypted, over a transmission medium (par 37), which *might* be a PSTN or other type of dedicated communications link such as an ISDN, DSL, T1, dedicated wireless connection or the like (par 42).

Therefore, based on the above arguments, the Examiner respectfully maintains the rejections as set forth below and amended to reflect the Applicant's amendments.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-4, 6, 8-11, 15-17, 20, 25-27, and 29-35 remain rejected under 35 U.S.C. 102(e) as being anticipated by Droge (U.S. Patent Application 09/841,168) and

Art Unit: 2137

Schneier (Applied Cryptography, 2nd ed.). Schneier has been relied upon as a reference for features inherent to the Data Encryption Standard (DES).

As per **claim 1**, Droge discloses a method for transmitting data over a wireless link to a gateway providing access to a wide area network, the method comprising: encrypting a payload according to a first encryption algorithm; adding a header to the encrypted payload to form a data packet; encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secure communication over the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; and transmitting the encrypted data packet over the wireless link (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

As per **claim 2**, Droge discloses the method of claim 1, wherein the first algorithm uses a symmetric key (see Droge paragraph 53 reference "DES").

As per **claim 3**, Droge discloses the method of claim 1, further comprising: receiving the data packet at the gateway; decrypting data packet at the gateway according to the second algorithm; forwarding the recovered data packet to a computer on the wide area network; and decrypting the payload at the computer on the wide area network according to the first algorithm (see Droge paragraphs 36-40 and 51).

As per **claim 4**, Droge discloses the method of claim 1, wherein the first algorithm uses a symmetric session key (see Droge paragraph 53 reference "DES").

As per **claim 6**, Droge discloses a device for transmitting data over a wireless link to a gateway providing access to a wide area network, comprising: a wireless transceiver (see Droge paragraph 36 and 40); and an encryption engine coupled to the wireless transceiver for encrypting a payload according to a first encryption algorithm, adding a header to the payload to form a data packet, and encrypting the data packet according to a second algorithm, the second encryption algorithm being an algorithm for secured communications over a wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding to the wide area network (see Droge paragraphs 12-13, 36-37, 39-42, and 50 and figures 5,6).

As per **claim 8**, Droge discloses the device of claim 6, wherein the payload comprises location information regarding the location of the wireless device (see Droge paragraph 58, reference "IP header").

As per **claim 9**, Droge discloses the device of claim 6, wherein the first encryption algorithm employs a symmetric key (see Droge paragraph 53 reference "DES").

As per **claim 10**, Droge discloses a method for secure communication between a mobile device (see Droge paragraphs 61-62) and a server (see Droge paragraph 60) on a wide area network, comprising: generating a symmetric session key at the mobile device; encrypting the symmetric session key at the mobile device using a public key

Art Unit: 2137

associated with the server; transmitting the encrypted session key to the server over a wireless link with a gateway to the wide area network; decrypting the encrypted session key at the server using a private key corresponding to the public key; encrypting a payload using the symmetric session key at the mobile device (see Droge paragraph 50 reference "algorithms that might be used to encrypt data at [the link layer] includes, without limitation, the DATA ENCRYPTION STANDARD (DES)"); adding a header to the payload to form a data packet at the mobile device; encrypting the encrypted payload and the header of the data packet using an encryption algorithm for secured communication over the wireless link to form an encrypted data packet at the mobile device, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; and transmitting the encrypted data packet from the mobile device to the gateway (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6, steps 92-102).

As per **claim 11**, Droge discloses the method of claim 10, further comprising: receiving the encrypted data at the gateway; decrypting the encrypted data packet at the gateway to recover a decrypted data packet, the decrypted data packet having the encrypted payload encrypted with the symmetric session key; forwarding the decrypted data packet to the server over the wide area network (see Droge figure 6, steps 104-114); decrypting the payload at the server using the decrypted session key (see Droge paragraph 50).

As per **claim 15**, Droge discloses the method of claim 10, wherein the payload includes location information (see Droge paragraph 58, reference "IP header").

As per **claim 16**, Droge discloses the method of claim 10, wherein the generating symmetric session key at the mobile device further comprises generating the symmetric key based on a random number (see Droge paragraph 53).

As per **claim 17**, Droge discloses the method of claim 10, wherein the encrypting a payload using the symmetric session key employs at least one of the encryption algorithms DESX or DES (see Droge paragraph 53).

As per **claim 20**, Droge discloses the method of claim 1, wherein the first algorithm comprises at least one of the encryption algorithms DES or DESX (see Droge paragraph 53).

As per **claim 25**, Droge discloses the method of claim 1, wherein the data packet includes location information (see Droge paragraph 58, reference "IP header").

As per **claim 26**, Droge discloses the method of claim 4, wherein the symmetric session key is generated based on a random number (see Droge paragraph 53).

As per **claim 27**, Droge discloses the device of claim 6 further comprising: a memory coupled to the encryption engine, the memory having a public key associated with a server on the wide area network stored therein (see Droge paragraph 39).

As per **claim 29**, Droge discloses a computer readable medium comprising program instructions for performing a method comprising: encrypting a payload according to a first encryption algorithm; adding a header to the encrypted payload to form a data packet; encrypting the encrypted payload and the header of the data packet

according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secure communications over a wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; transmitting the data packet to a server on a wide area network over a wireless link with a gateway providing access to the wide area network (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

As per **claim 30**, Droge discloses the computer readable medium of claim 29, wherein the first algorithm uses a symmetric key (see Droge paragraph 53 reference "DES").

As per **claim 31**, Droge discloses the computer readable medium of claim 29, the method further comprising: receiving the data packet at the gateway; decrypting the data packet at the gateway according to the second algorithm; forwarding the recovered data packet to a computer on the wide area network; and decrypting the payload at the computer on the wide area network according to the first algorithm (see Droge paragraphs 36-40 and 51).

As per **claim 32**, Droge discloses the computer readable medium of claim 29, wherein the first algorithm uses a symmetric session key (see Droge paragraph 53 reference "DES").

As per **claim 33**, Droge discloses the computer readable medium of claim 29, wherein the first algorithm comprises at least one of the encryption algorithms DESX or DES (see Droge paragraph 53).

As per **claim 34**, Droge discloses the computer readable medium of claim 29 wherein the data packet includes location information (see Droge paragraph 58, reference "IP header").

As per **claim 35**, Droge discloses the computer readable medium of claim 32 wherein the symmetric session key is generated based on a random number (see Droge paragraph 53).

Conclusion

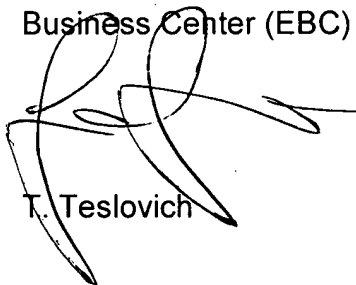
THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

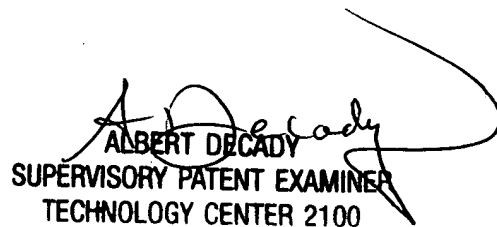
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



T. Teslovich



ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100